IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PATRICK REYNOLDS, *et al.*, Plaintiffs, v. **MARYMOUNT MANHATTAN COLLEGE,** Defendant.	Case No. 1:22-cv-06846 JUDGE LORNA G. SCHOFIELD **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Patrick Reynolds, Daniel Lewis, Lucia Marano, Kristen France, Abbey Abrecht, and Jahidah Diaab ("Plaintiffs") bring this Consolidated Class Action Complaint against Marymount Manhattan College ("MMC" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant MMC, a private college located in New York City, New York. Defendant failed to implement and maintain reasonable data security measures, such as standard encryption or redaction of sensitive data, leading to the theft of the sensitive personal information of Plaintiffs and more than 191,000 other current and former students, admission applicants, employees of MMC, and others who entrusted Defendant with their most sensitive data. Plaintiffs seek damages on behalf of themselves and Class Members, as well as equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiffs and Class Members.

2. Prior to and through November 12, 2021, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on

Defendant's network.

3. Defendant's Privacy Statement (the "Privacy Statement"), posted on its website, represents that it "provides a secure server to protect [students'] information. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure information. The Information Technology department at Marymount Manhattan employs various measures to protect the security of its computing resources and its users' accounts."[1]

4. In Defendant's Information Technology Policy (the "Information Technology Policy"), posted on its website, Defendant "recognizes that global access to information provides many opportunities but also many challenges. The commercialization and ubiquity of the internet has allowed hackers, virus writers and professional criminals to attack free and open academic networks."[2]

5. Defendant's Information Security Plan (the "Information Security Plan"), posted on its website, provides that "covered data," including Social Security numbers, will be protected by "reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly."[3]

6. The specific data exposed—and then stolen—was a variety of personally identifiable information ("PII") and protected health information ("PHI"). Specifically, Defendant lost control of credit card information, payment information, student IDs, employee IDs, dates of

[1] *See* https://www.mmm.edu/offices/information-technology/mmc-privacy-statement/ (last accessed Aug. 16, 2022) (attached hereto as **Exhibit 1**).
[2] *See* § 1, *available at* https://www.mmm.edu/offices/information-technology/information-security-policy/ (last accessed Aug. 16, 2022) (attached hereto as **Exhibit 2**).
[3] *See* §§ 2, 4.3, *available at* https://www.mmm.edu/offices/human-resources/information-security-program.php (last accessed Aug. 16, 2022) (attached hereto as **Exhibit 3**).

birth, medical information, health insurance information, and Social Security numbers.[4] Defendant also admitted that "other types of information" were exposed.[5] Thus, the exposure may extend to data types not specifically listed above. The PII and PHI that Defendant collected and maintained will be collectively referred to as the "Private Information."

7. MMC failed to provide timely, accurate and adequate notice to Plaintiffs and Class Members, who are past and present students, employees, parents, and applicants to MMC. Plaintiffs' and Class Members' knowledge about the Private Information MMC lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by MMC's failure to warn impacted persons for approximately nine-month after first learning of the data breach.

8. On or about August 3, 2022, MMC finally notified state Attorneys General and many Class Members about a widespread data breach in which the sensitive Private Information of individuals was accessed and acquired by a malicious actor. MMC explained in its required notice letter that it discovered *on November 12, 2021* (almost nine months earlier) that it "experienced a network disruption" and that files on its network were accessed and acquired by the unknown actor (the "Data Breach").[6]

9. MMC admitted it experienced a "network disruption" on November 12, 2021, and "the MMC IT team, working in concert with cybersecurity experts, immediately determined that

---

[4] *Cybersecurity*, MARYMOUNT MANHATTAN, https://www.mmm.edu/offices/information-technology/cybersecurity/ (last accessed Oct. 10, 2022); *Data Security Breach Reports*, OFFICE OF THE ATTORNEY GENERAL OF TEXAS, https://oagtx.force.com/datasecuritybreachreport /apex/ DataSecurityReportsPage (last accessed Oct. 6, 2022) (listing "Medical Information; Health Insurance Information" as among the "type(s) of information affected").

[5] *Cybersecurity*, MARYMOUNT MANHATTAN, https://www.mmm.edu/offices/information-technology/cybersecurity/ (last accessed Oct. 10, 2022).

[6] Office of the Vermont Attorney General, https://ago.vermont.gov/blog/2022/08/03/marymount-manhattan-college-data-breach-notice-to-consumers/ (last accessed Aug. 9, 2022) (hereafter "Notice Letter").

the network had been accessed without authorization." [7]

10. An unknown threat actor accessed the system using MMC's "IT network vulnerability" that is "a very common method used for cyberattacks." Once in the system, a remote desktop application was used to access files on some of MMC's servers.[8]

11. While the Data Breach occurred in November 2021, MMC chose not to notify affected individuals or, upon information and belief, anyone of its Data Breach instead choosing to address the incident in-house by implementing unknown safeguards to some unidentified aspects of its computer security. It then, without warning persons impacted by the Data Breach, simply resumed its normal business operations.

12. Defendant posted a notice on its website (the "Website Notice") advising that the Private Information impacted included student ID, date of birth, Social Security Number, employee ID, payment and credit card information, and some other types of information.[9]

13. Upon determining that the breach occurred, MMC began working with external cyber and legal experts to investigate and respond to the unauthorized access and strengthen MMC's IT network.[10]

14. MMC has admitted it has since had to install new cybersecurity software on its systems and devices, implement additional authentication protocols for systems, applications, and remote network access, and it initiated a global password reset for the entire community.[11]

15. Over eight months later, on July 28, 2022, MMC claims it concluded its

---

[7] *Cybersecurity*, Marymount Manhattan, https://www.mmm.edu/offices/information-technology/cybersecurity/ (last accessed October 10, 2022).
[8] *Id.*
[9] https://www.mmm.edu/offices/information-technology/cybersecurity/ (last accessed Aug. 16, 2022) (attached hereto as **Exhibit 4**).
[10] *Id.*
[11] *Id.*

investigation and determined that Plaintiffs' and Class Members' Private Information had been impacted and taken from its network.[12]

16. MMC still took nearly a week to notify state Attorneys General and Class Members about the widespread Data Breach.[13]

17. According to the Notice Letter it sent Attorneys General and some Class Members, MMC "secure[d] the network environment," hired "cybersecurity experts" to investigate the breach of MMC's systems, and determined that Plaintiffs' and Class Members' Private Information (including but not limited to full names and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident.[14]

18. MMC's Notice Letter plainly admits that Plaintiffs' and Class Members' Private Information were compromised when the "unknown actor gained access to and obtained data from the MMC network without authorization."[15] This means that Plaintiffs' and Class Members' Private Information was exfiltrated by the unauthorized actors during the Data Breach.

19. Plaintiffs and Class Members first learned of the November 2021 Data Breach when they received Data Breach notice letters dated August 3, 2022, via regular U.S. mail directly from MMC.

20. In its Notice Letters, sent to state and federal agencies and some Class Members, MMC failed to explain why it took the company nearly nine months (from November 12, 2021, when MMC detected unusual activity to August 3, 2022) to alert Class Members that their sensitive

[12] Office of the Vermont Attorney General, *https://ago.vermont.gov/blog/2022/08/03/marymount-manhattan-college-data-breach-notice-to-consumers/* (last accessed Aug. 9, 2022) (hereafter "Notice Letter").
[13] *Id.*
[14] *Id.*
[15] *Id.*

Private Information had been exposed.[16] As a result of this delayed response, Plaintiffs and Class Members were unaware that their Private Information had been compromised, and that they were, and continue to be, at a present and significant risk of identity theft and various other forms of personal, social, and financial harm.

21. Further, MMC's letters noticing some Plaintiffs and certain Class Members do not explain the precise scope of the Data Breach or how long the unauthorized actor had access to Defendant's network.[17] In fact, the letters Plaintiffs received are markedly different from those that Defendant provided to the Attorneys General offices. Plaintiffs' letters simply state:

> Marymount Manhattan College ("MMC") is writing to inform you about an information security incident that involved your personal information. We are writing to inform you of the incident and to advise you of certain steps that you can take to help protect your personal information.

22. The letter provides no further information regarding the Data Breach and only goes on to recommend how to place a security freeze on a credit report and how to sign up for the identity monitoring services Defendant offered in response to the Data Breach. The letters Plaintiffs and other Class Members received do not explain when or how the Data Breach occurred, when MMC detected the Data Breach, what steps MMC took following the Data Breach, or most importantly, which of Plaintiffs' Private Information was impacted by the Data Breach. It is wholly different from the Notice Letters sent to state Attorneys General.

23. Plaintiffs' and Class Members' unencrypted, unredacted Private Information was compromised due to MMC's negligent and/or careless acts and omissions, and due to its utter failure to protect Class Members' sensitive data. Hackers targeted and obtained the Private Information because of its value in exploiting and stealing the identities of Plaintiffs and similarly

[16] Notice Letter
[17] *Id.*

situated Class Members. The risks to these persons will remain for their respective lifetimes.

24. Defendant failed to undertake adequate cybersecurity practices, including but not limited, to, maintaining the Private Information in an unencrypted format and failing to adhere to routine cybersecurity protocols and procedures.

25. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised due to MMC's failure to: (i) adequately protect Plaintiffs' and Class Members' Private Information; (ii) warn Plaintiffs and Class Members of its inadequate information security practices; and (iii) effectively monitor MMC's network for security vulnerabilities and incidents. MMC's conduct amounts at least to negligence and violates federal and state statutes.

26. Plaintiffs and Class Members have suffered injuries due to MMC's conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) loss of privacy (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (v) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (vi) charges and fees associated with fraudulent charges on their accounts, and (vii) the present, continued, and certainly an increased risk to their Private Information, which remains in MMC's possession and is subject to further unauthorized disclosures so long as MMC fails to undertake appropriate and adequate measures to protect the Private Information. These risks will remain for the lifetimes of Plaintiffs and Class Members.

27. MMC disregarded the rights of Plaintiffs and Class Members by intentionally,

willfully, recklessly, or at the very least negligently, failing to take and implement adequate and reasonable measures to ensure that Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, Plaintiffs' and Class Members' Private Information was compromised through disclosure to unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

I. PARTIES

Plaintiff Patrick Reynolds

28. Plaintiff Patrick Reynolds is a resident and citizen of Massachusetts, residing in Hudson, Massachusetts. Mr. Reynolds received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by U.S. Mail.

Plaintiff Daniel Lewis

29. Plaintiff Daniel Lewis is a resident and citizen of Connecticut, residing in Westport, Connecticut. Mr. Lewis received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by U.S. Mail.

Plaintiff Lucia Marano

30. Plaintiff Lucia Marano is a resident and citizen of New York, residing in Yonkers, New York. Ms. Marano received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by U.S. Mail.

Plaintiff Kristen France

31. Plaintiff Kristen France is a resident and citizen of New York, residing in Forest

Hills, New York. Ms. France received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by US. Mail.

Plaintiff Abbey Abrecht

32. Plaintiff Abbey Abrecht is a resident and citizen of California, residing in Aliso Viejo, California. Ms. Abrecht received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by US. Mail.

Plaintiff Jahidah Diaab

33. Plaintiff Jahidah Diaab is a resident and citizen of New York, residing in Niagara Falls, New York. Ms. Diaab received a Notice of Data Security Incident letter from MMC, dated August 3, 2022, by U.S. Mail.

Defendant Marymount Manhattan College

34. Defendant MMC is a private college located in New York City, New York, which has a principal place of business at 221 East 71st Street, New York, New York 10021.

35. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

36. All of Plaintiffs' claims stated herein are asserted against MMC and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

II. JURISDICTION AND VENUE

37. This Court has original subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). First, because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. Second, because this class action involves a putative

class of over 100 members. And third, because there is sufficient diversity—while Defendant's principal place of business is in New York, many Class Members are citizens of different states.

38. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in New York City, New York, and Defendant regularly conducts business in New York.

39. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

III. FACTUAL ALLEGATIONS

Background

40. MMC is a private college located in New York City, New York, which has a principal place of business at 221 East 71st Street, New York, New York 10021.

41. In its Notice Letters sent to Attorneys General, MMC claims that it "takes the privacy and security of the personal information in our possession very seriously."

42. On its own website, MMC holds itself out as committed to protecting the privacy of its students. MMC states it "does not sell, rent, give away or loan any identifiable information to any third party other than agents and contractors of MMC."[18]

43. MMC's Privacy Statement provides:

> MMC provides a secure server to protect your information. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure information. The Information Technology department at Marymount Manhattan employs various measures to protect the security of its computing resources and its users' accounts.[19]

[18] Exhibit 1.
[19] *Id.*

44. In the Information Technology Policy, Defendant represents that it "will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives," including as to "[a]ll information stored on applicable information systems."[20]

45. In the Information Technology Policy, Defendant represents that it "safeguards the privacy of students, employees, College business, and other matters by protecting electronic records classified as confidential information."[21]

46. In the Information Technology Policy, Defendant recognizes that it "should gather as little information as possible for legitimate purposes and delete information when it is no longer needed or no longer required by law to be retained."[22]

47. In the Information Technology Policy, Defendant recognizes that "[a] breach of data security that compromises personal information can lead to identity theft, putting members of the MMC community at risk and exposing the College to litigation."[23]

48. As MMC acknowledges in its Notice Letters, protection of personally identifiable information is something it takes "very seriously."

49. Plaintiffs and the Class Members, as current or former students, applicants, parents of the same, or employees of MMC, reasonably relied (directly or indirectly) on this sophisticated higher education institution to keep their sensitive Private Information confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information. People demand security to safeguard their Private Information, especially when Social Security numbers, financial account numbers and sensitive

[20] Exhibit 2, § 1.4.
[21] *Id.* § 17.
[22] *Id.* § 17.7.
[23] *Id.* § 18.

PHI is involved as here.

50. MMC had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

51. Defendant knows that a data breach causes serious injury. After all, Defendant states that "[a] breach in data security that compromises personal information can lead to identity theft, putting members of MMC community at risk."[24]

Defendant Fails to Secure the Private Information, Resulting in a Data Breach

52. In early August 2022, MMC first began notifying Class Members and state Attorneys General ("AGs") about a widespread breach of its computer systems and involving the sensitive personal identifiable information of "past and current students, employees, parents, and applicants to MMC."[25] MMC explained that the Data Breach was detected in November 2021.[26]

53. According to its August 3, 2022, Notice Letters notifying state AGs and many impacted persons of the breach, MMC discovered *on November 12, 2021* (nearly nine months earlier) that it "experienced a network disruption," involving a widespread data breach of the sensitive Private Information of thousands of individuals. MMC discovered that files on its network were accessed and acquired by the unknown actor.

54. The delay between the breach and the notifications was unreasonable. Even Defendant itself admits that "the time between the incident and notification is greater than any of

[24] Exhibit 3.
[25] Office of the Vermont Attorney General, *https://ago.vermont.gov/blog/2022/08/03/marymount-manhattan-college-data-breach-notice-to-consumers/* (last accessed Aug. 9, 2022); https://www.mmm.edu/offices/information-technology/cybersecurity/.
[26] *Id.*

us would prefer."[27]

55. Still, Defendant states that it "deeply regrets any worry or inconvenience" that its data breach caused to "members of our community."[28] Then, Defendant told its community members to direct their concerns and questions to a call center—that is closed on weekends, and only open during select hours on weekdays.[29]

56. In November 2021, MMC chose not to notify affected individuals or, upon information and belief, anyone, of its Data Breach instead choosing to address the incident in-house by implementing unknown safeguards to some aspects of its computer security. It then simply resumed its normal business operations.

57. Over eight months later, on July 28, 2022, MMC concluded its investigation and finally admitted that Plaintiffs' and Class Members' Private Information had been impacted and taken from its network.[30]

58. MMC hired "cybersecurity experts" and "secure[d] the network environment" of MMC's systems and determined that Plaintiffs' and Class Members' Private Information (including but not limited to full names and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident. [31]

59. Plaintiffs and Class Members in this action were, according to MMC, current, former, and prospective students at MMC, their parents, and MMC employees. The first time that Plaintiffs and Class Members learned of the Data Breach was nearly nine months after MMC learned of the Data Breach. MMC has still not disclosed to Plaintiffs and Class Members the full

[27] Marymount Manhattan College, *Cybersecurity*, https://www.mmm.edu/offices/information-technology/cybersecurity/ (last accessed Oct. 10, 2022).
[28] *Id*.
[29] *Id*.
[30] *Id.*
[31] *Id.*

scope of the Data Breach or precisely what information was impacted. MMC's letters to Plaintiffs simply states there was, "an information security incident that involved your personal information. We are writing to inform you of the incident and to advise you of certain steps that you can take to help protect your personal information." The letter offers Plaintiffs no further details about the personal information at issue.

60. According to MMC's website, the confidential information that was accessed without authorization included at least names, Social Security numbers, student IDs, date of birth, social security numbers, employee IDs, "as well as some other types of information," including payment and credit card information.

61. Upon information and belief, the Private Information was not encrypted prior to the data breach.

62. Upon information and belief, the cyberattack was targeted at MMC as a higher education institution that collects and maintains valuable personal, health, tax, and financial data.

63. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) Plaintiffs' and Class Members' Private Information.

64. MMC admitted in its Notice Letter to the Attorneys General that its systems were subjected to unauthorized access in November 2021. In the Notice Letters, MMC made no indication to either group (AGs or Class) that the exfiltrated Private Information was retrieved from the cybercriminals who took it, nor how long the data was available to these unauthorized actors.[32]

[32] *See* Notice Letter.

65. With its offer of credit and identity monitoring services to victims, MMC is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud as a result of its failure to protect the Private Information it collected and maintained.

66. In response to the Data Breach, MMC claims that "additional security features were also implemented to reduce the risk of a similar incident occurring in the future."[33] MMC admits additional security was required, but there is no indication what these measures entail and whether these steps are adequate to protect Plaintiffs' and Class Members' Private Information going forward.

67. MMC had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep the Private Information that was entrusted to MMC confidential, and to protect the Private Information from unauthorized access and disclosure.

68. Plaintiffs and Class Members provided their Private Information to MMC with the reasonable expectation that MMC as a higher education institution would comply with its duties, obligations, and representations to keep such information confidential and secure from unauthorized access.

69. MMC failed to uphold its data security obligations to Plaintiffs and Class Members. As a result, Plaintiffs and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

70. MMC did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiffs' and Class

[33] *Id*.

Members' Private Information to be exposed.

71. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[34]

72. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

[34] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Aug. 23, 2021).

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[35]

73. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact

[35] *Id.* at 3-4.

information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[36]

74. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities

[36] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Aug. 23, 2021).

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[37]

75. Given that Defendant was storing the Private Information of more than 191,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

76. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of more than 191,000 individuals, including Plaintiffs and Class Members.

Securing Private Information and Preventing Breaches

77. MMC could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

78. In its notice letters, MMC acknowledged the sensitive and confidential nature of the Private Information. To be sure, collection, maintaining, and protecting Private Information is vital to virtually all of MMC's business purposes as a private higher education institution. MMC acknowledged through its conduct and statements that the misuse or inadvertent disclosure of Private Information can pose major privacy and financial risks to impacted individuals, and that

[37] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Aug. 23, 2021).

under state law they may not disclose and must take reasonable steps to protect Private Information from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

79. It is well known that Private Information, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

80. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[38]

81. "Since 2005, K–12 school districts and colleges/universities across the US have experienced over 1,850 data breaches, affecting more than 28.6 million records."[39]

82. In 2020 alone, approximately 2.99 million records from educational institutions were subject to data breaches.[40]

83. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

84. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers

[38] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Oct. 11, 2022).
[39] Sam Cook, US schools leaked 28.6 million records in 1,851 data breaches since 2005, https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/ (last accessed Oct. 11, 2022).
[40] *Id.*

have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

85. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), MMC knew or should have known that its electronic records would be targeted by cybercriminals.

86. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

87. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep Private Information private and secure, MMC failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

88. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

89. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that,

among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[41]

90. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[42]

91. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[43]

92. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web

---

[41] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed Jan. 25, 2022).

[42] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed Jan. 25, 2022).

[43] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last accessed Jan. 25, 2022).

portals, and (iv) ransomware tactics included threatening to release stolen data.

93. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of more than 191,000 individuals in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

94. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack.

95. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

At All Relevant Times MMC Had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information

96. At all relevant times, MMC had a duty to Plaintiffs and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to *promptly* notify Plaintiffs and Class Members when MMC became aware that their Private Information may have been compromised.

97. MMC's duty to use reasonable security measures arose as a result of the special relationship that existed between MMC, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class entrusted MMC with their Private Information as a condition of receiving educational services for

themselves or their children or when they applied for or accepted employment at MMC.

98. MMC had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, MMC breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

99. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

100. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[44] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[44] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[45]

101. The ramifications of MMC's failure to keep Plaintiffs' and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Private Information

102. Stolen personal information is one of the most valuable commodities on the information black market. According to Experian, a credit-monitoring service, stolen personal information can sell for over $1,000.00 (depending on the type of information).[46]

103. The value of Plaintiffs' and Class Members' personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites. Thus, after charging a substantial fee, criminals make such stolen information publicly available.

104. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[47] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[48]

---

[45] *Id*.
[46] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[47] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[48] *See* https://datacoup.com/ (last accessed Oct. 21, 2022).

105. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

106. By failing to properly notify Plaintiffs and the Class Members of the Data Breach, Defendant exacerbated their injuries. Specifically, by depriving them of the chance to take speedy measures to protect themselves and mitigate harm, Defendant allowed their injuries to fester and the damage to spread.

107. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[49]

108. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and

[49] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 10, 2021).

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

109. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[50]

110. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[51]

111. Defendant recognizes the value and importance of Social Security numbers. Its' website discusses how "[m]any people do not realize the importance of Social Security numbers and what can happen when their number gets into the hands of the wrong people."[52] Further, Defendant recognizes that "[y]our Social Security number is your personal property."[53]

112. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an

---

[50] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Dec. 10, 2021).

[51] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 10, 2021).

[52] *Social Security Information*, MARYMOUNT MANHATTAN COLLEGE, https://www.mmm.edu/offices/human-resources/social-security-information.php (last accessed Oct. 7, 2022).

[53] *Id*.

individual, such as their birthdate, birthplace, and mother's maiden name.[54]

113. It can take years for victims to notice their identity was stolen—giving criminals plenty of time to sell one's personal information to the highest bidder.

114. One example of criminals using Private Information for profit is the development of "Fullz" packages.

115. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

116. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

117. That is exactly what is happening to Plaintiffs and Class Members. And it is reasonable for any trier of fact, including this Court or a jury, to find that the stolen Private Information (of Plaintiffs and the other Class Members) is being misused—and that such misuse is fairly traceable to Defendant's data breach.

118. Over the past several years, data breaches have become alarmingly common. In 2016, the number of data breaches in the U.S. exceeded 1,000—a 40% increase from 2015.[55] The next year, that number increased further by nearly 45%.[56]

---

[54] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[55] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed Aug. 15, 2022).

[56] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018),

119. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets—so that they are aware of, and prepared for, a potential attack. One report explained that smaller entities "are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[57]

120. Thus, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry—including Defendant.

121. Responsible for handling highly sensitive personal information, Defendant knew or should have known the importance of safeguarding Private Information. Defendant also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on victims of the breach. Still, Defendant failed to take adequate measures to prevent the data breach.

122. Because of Defendant's inadequate practices, the Private Information of Plaintiffs and the Class was exposed to criminals. In other words, Defendant opened up, disclosed, and then exposed its Private Information to crooked operators and criminals. Such criminals engage in disruptive and unlawful business practices and tactics, like online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud)—all using stolen Private Information.

123. Given the nature of MMC's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised Private Information has been or will be

---

https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed Aug. 15, 2022).

[57] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed Aug. 15, 2022).

used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

124. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, simple credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[58] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

125. To date, MMC has offered Plaintiffs and Class Members *only one or two years* of identity monitoring services despite the almost nine-month delay from their discovery of the Data Breach to the Notice Letters. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

126. The injuries to Plaintiffs and Class Members were directly and proximately caused by MMC's failure to implement or maintain adequate data security measures to protect Private Information that it maintained.

MMC Failed to Comply with FTC Guidelines

127. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

[58] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1_(last accessed Dec. 10, 2021).

business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[59]

128. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[60] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

129. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[61]

130. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or

---

[59] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 10, 2021).

[60] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 10, 2021).

[61] FTC, *Start with Security*, *supra* note 59.

an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

131. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

132. Because Class Members entrusted MMC with their Private Information directly or indirectly through MMC, MMC had, and has, a duty to the Class Members to keep their Private Information secure.

133. Plaintiffs and the other Class Members reasonably expected that when they provide Private Information to their college, that MMC would safeguard their Private Information.

134. MMC was at all times fully aware of its obligation to protect the personal data of Students, including Plaintiffs and members of the Classes. MMC was also aware of the significant repercussions if it failed to do so.

135. MMC's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiffs' and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiffs and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

136. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

137. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit

of their bargain. When agreeing to pay Defendant for their education, Plaintiffs and other Class Members reasonably understood and expected that their Private Information would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

138. Cybercriminals target and capture Private Information to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

139. The cybercriminals who targeted and obtained Plaintiffs' and Class Members' Private Information may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other Private Information, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

140. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

141. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their Private Information, for which there is a well-established national and international market.

142. Furthermore, certain Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[62]

143. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[63] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[64] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[65] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

144. As a result of the Data Breach, Plaintiffs and Class Members have already suffered

---

[62] *Id.*

[63] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (Feb. 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed Dec. 10, 2021).

[64] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed Dec. 10, 2021).

[65] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Dec. 10, 2021).

damages.

145. In its Notice Letter, Defendant represented to the AGs that it initially discovered the Data Breach on November 12, 2021, and admitted files were accessed and acquired by the cybercriminals.

146. In this case, according to Defendant's notification to the state Attorneys General, cybercriminals had access to and acquired Class Members' data at least on November 12, 2021, yet its notice letters about that Data Breach did not go out until August 3, 2022.

147. Because of this nearly nine-month delay, cybercriminals had plenty of time to sell Plaintiffs' and Class Members' data on the black market. Simply put, the delay between the breach and the notifications was unreasonable and compounded the harm to Plaintiffs and Class Members.

Plaintiff Patrick Reynolds's Experience

148. On or about August 3, 2022, Plaintiff Patrick Reynolds, a citizen and resident of Hudson, Massachusetts, received a Notice of Data Security Incident Letter by US. Mail. The letter Plaintiff Reynolds received lacked any detail about the scope of the Data Breach, which of his Private Information was involved, when the Data Breach was detected, or what steps, if any, that Defendant took in response to the Data Breach. The letter Plaintiff Reynolds received was markedly different from the Notice Letter sent to the Attorneys General.

149. When applying for admission and while a student at MMC, Plaintiff Reynolds provided his Private Information to MMC to gain admission, financial aid, and receive his education, which he was required to do under state and federal law. He reasonably relied on MMC to protect the security of his Private Information.

150. As a result of the Data Breach and the information that he received in the letter, Mr. Reynolds has spent many hours dealing with the consequences of the Data Breach (considering

closing and opening bank accounts, changing banks, changing passwords, and now self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice Letter, communicating with MMC representatives, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured and time that he could have spent on other pursuits like work or leisure activities.

151. Mr. Reynolds is very careful about sharing his own personal identifying information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

152. Mr. Reynolds stores any and all documents containing Private Information in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

153. Mr. Reynolds suffered actual injury and damages due to MMC's mismanagement of his Private Information before the Data Breach.

154. Mr. Reynolds suffered actual injury in the form of damages and diminution in the value of his Private Information, a form of intangible property that he entrusted to MMC, which was compromised in and as a result of the Data Breach.

155. Mr. Reynolds suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered extreme anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

156. Mr. Reynolds has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

157. Mr. Reynolds has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

Plaintiff Daniel Lewis's Experience

158. On or about August 3, 2022, Mr. Daniel Lewis, a citizen and resident of Westport, Connecticut, received a Notice of Data Security Incident Letter by US. Mail. The letter Mr. Lewis received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Mr. Lewis's name and Social Security number were accessed and acquired in the Data Breach.

159. When applying for admission and while a student at MMC, Mr. Lewis provided his Private Information to MMC in order to gain admission, financial aid, receive his education, and under state and federal law, he was required to do so. He reasonably relied on MMC, a higher education institution, to protect the security of his Private Information.

160. Following the Data Breach, Mr. Lewis has suffered multiple instances of fraud and identity theft including an unauthorized charge of $850 on one of his payment cards.

161. As a result of the Data Breach and the information that he received in the letter, Mr. Lewis has spent many hours dealing with the consequences of the Data Breach (considering closing and opening bank accounts, changing banks, changing passwords, and now self-

monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice Letter, communicating with MMC representatives, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured and time that he could have spent on other pursuits like work or leisure activities.

162. Mr. Lewis is very careful about sharing his own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

163. Mr. Lewis stores any and all documents containing Private Information in a secure location, and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

164. Mr. Lewis suffered actual injury and damages due to MMC's mismanagement of his Private Information before the Data Breach.

165. Mr. Lewis suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to MMC, which was compromised in and as a result of the Data Breach.

166. Mr. Lewis suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered extreme anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

167. Mr. Lewis has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

168. Mr. Lewis has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

Plaintiff Lucia Marano's Experience

169. On or about August 3, 2022, Ms. Lucia Marano, a citizen and resident of Yonkers, New York received a Notice of Data Security Incident Letter by US. Mail. The letter Ms. Marano received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Ms. Marano's name and Social Security number were accessed and acquired in the Data Breach.

170. When applying for admission and while a student at MMC from 1995 to 2000, Ms. Marano provided her Private Information to MMC in order to gain admission, financial aid, receive her education, and under state and federal law, she was required to do so. She reasonably relied on MMC, a higher education institution, to protect the security of her Private Information.

171. As a result of the Data Breach, Plaintiff Marano's sensitive information was acquired by an unauthorized actor. The confidentiality of Plaintiff Marano's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Marano will have to worry about when and how her sensitive information may be shared or used to her detriment.

172. As a result of the Data Breach notice, Plaintiff Marano spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Data Security Incident and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

173. Additionally, Plaintiff Marano is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

174. Plaintiff Marano stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

175. Plaintiff Marano suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

176. Plaintiff Marano has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

177. Plaintiff Marano has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kristen France's Experience

178. On or about August 3, 2022, Ms. Kristen France, a citizen and resident of Forest Hills, New York received a Notice of Data Security Incident Letter by US. Mail. The letter Ms. France received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Ms. France's name and Social Security

number were accessed and acquired in the Data Breach.

179. When applying for admission at MMC in 2018, Ms. France provided her Private Information to MMC in order to gain admission and qualify for financial aid, and under state and federal law, she was required to do so. She reasonably relied on MMC, a higher education institution, to protect the security of her Private Information. Plaintiff France chose not to attend or enroll in MMC.

180. Following the Data Breach, Plaintiff France's finances and financial accounts were attacked by unauthorized fraudulent actors who attempted to open fraudulent accounts in Plaintiff France's name.

181. Plaintiff France, who maintains full-time employment and is a full-time student, has been forced to deal with the numerous issues caused by the barrage of attempted fraud and attempted theft on her accounts.

182. Following the Data Breach, an unauthorized person attempted to fraudulently take out a loan of $10,000 in Plaintiff France's name. Plaintiff France was able to cancel the loan after discovering the fraud.

183. As a result of the attempted fraud, Plaintiff France froze her credit to stop future potential abuses.

184. After freezing her credit, another unauthorized person attempted to open a Chase credit card under Plaintiff France's name. Plaintiff France was able to stop the credit card from being issued.

185. Additionally, following the Data Breach, Plaintiff France discovered that her Private Information was found on the Dark Web.

186. Plaintiff France's Private Information can be purchased by criminals intending to

utilize the PII for identity theft crimes, such as opening bank accounts in her name to make purchases or to launder money; filing false tax returns; or filing false unemployment claims. Plaintiff France believes that the availability of her Private Information on the dark web is directly related to the Data Breach.

187. Plaintiff France has also experienced a substantial increase in suspicious emails and "spam" telephone calls since the Data Breach which she believes were a result of the Data Breach.

188. As a result of the Data Breach and the information that she received in the Notice Letter, Plaintiff France has spent many hours dealing with the consequences of the Data Breach (monitoring bank accounts, changing passwords, and now self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the *Notice of Data Security Incident*, communicating with MMC representatives, and communicating with her bank and payment card providers. This time has been lost forever and cannot be recaptured.

189. Plaintiff France is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Prior to the Data Breach, Plaintiff France enrolled in credit monitoring services from TransUnion.

190. Plaintiff France stores any and all documents containing Private Information in a secure location, and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

191. Plaintiff France suffered actual injury and damages due to MMC's mismanagement of her PII before the Data Breach.

192. Plaintiff France suffered concrete and substantial injuries as a result of fraudulent attacks on Plaintiff France's financial accounts and identify that occurred when her Private Information was compromised in and as a result of the Data Breach.

193. Plaintiff France suffered actual injury in the form of damages and diminution in the value of her Private Information, a form of intangible property that she entrusted to MMC, which was compromised in and as a result of the Data Breach.

194. Plaintiff France suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered extreme anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

195. Plaintiff France has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

196. Plaintiff France has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

Plaintiff Abbey Abrecht's Experience

197. On or about August 3, 2022, Ms. Abbey Abrecht, a citizen and resident of Aliso Viejo, California received a Notice of Data Security Incident Letter by US. Mail. The letter Ms. Abrecht received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Ms. Abrecht's name and Social Security

number were accessed and acquired in the Data Breach.

198. As a student at MMC from 2013 until her graduation in 2017, Ms. Abrecht provided her Private Information to MMC in order to gain admission, financial aid, receive her education, and under state and federal law, she was required to do so. She reasonably relied on MMC, a higher education institution, to protect the security of her Private Information.

199. Following the Data Breach, Plaintiff Abrecht received notice from Experian that her Private Information was found on the Dark Web.

200. Plaintiff Abrecht's Private Information can be purchased by criminals intending to utilize the Private Information for identity theft crimes, such as opening bank accounts in her name to make purchases or to launder money; filing false tax returns; or filing false unemployment claims. Plaintiff Abrecht believes that the availability of her Private Information on the dark web is directly related to the Data Breach.

201. In addition, Plaintiff Abrecht has also experienced a substantial increase in suspicious emails and "spam" telephone calls since the Data Breach which she believes were a result of the Data Breach.

202. As a result of the Data Breach and the information that she received in the Notice Letter, Plaintiff Abrecht has spent many hours dealing with the consequences of the Data Breach (monitoring bank accounts, changing passwords, and now self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice of Data Security Incident, communicating with MMC representatives, communicating with her bank, and signing up for the credit monitoring supplied by MMC. This time has been lost forever and cannot be recaptured.

203. Plaintiff Abrecht is very careful about sharing her own personal identifying

information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Prior to the Data Breach, Plaintiff Abrecht enrolled in credit monitoring services from Intuit. She also enrolled in account monitoring services from her bank.

204. Plaintiff Abrecht stores any and all documents containing Private Information in a secure location, and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

205. Plaintiff Abrecht suffered actual injury and damages due to MMC's mismanagement of her Private Information before the Data Breach.

206. Plaintiff Abrecht suffered actual injury in the form of damages and diminution in the value of her Private Information, a form of intangible property that she entrusted to MMC, which was compromised in and as a result of the Data Breach.

207. Plaintiff Abrecht suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered extreme anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

208. Plaintiff Abrecht has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

209. Plaintiff Abrecht has a continuing interest in ensuring that her Private Information,

which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

Plaintiff Jahidah Diaab Experience

210. On or about August 3, 2022, Ms. Jahidah Diaab a citizen and resident of Niagara Falls, New York received a Notice of Data Security Incident Letter by US. Mail. The letter Ms. Diaab received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Ms. Diaab's name and Social Security number were accessed and acquired in the Data Breach.

211. As a former student at MMC, Ms. Diaab provided her Private Information to MMC in order to gain admission, financial aid, receive her education, and under state and federal law, she was required to do so. She reasonably relied on MMC, a higher education institution, to protect the security of her Private Information.

212. Defendant inflicted numerous actual injuries and damages upon Plaintiff Diaab — all because Defendant failed to properly secure her Private Information.

213. Because of the data breach notice, Plaintiff Diaab expended a great deal of time trying to mitigate the fallout of Defendant's misconduct. Plaintiff Diaab has expended time, *inter alia*, verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts, and checking her credit reports for fraudulent activity.

214. Such expenditures of time cannot be recouped. In other words, Defendant deprived Plaintiff Diaab of the opportunity to direct her time to more meaningful pursuits like leisure or work.

215. Plaintiff Diaab has spent—and will continue to spend—considerable time and

effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Diaab fears for her personal financial security. And now she must deal with uncertainty of not knowing exactly how much Defendant exposed her to criminals.

216. Plaintiff Diaab has experienced—and will continue to experience—anxiety, sleep disruption, stress, fear, and frustration because of the data breach. This goes far beyond allegations of mere worry or inconvenience. Rather, it is precisely the type of injuries and harm to a data breach victim that the law contemplates and addresses.

217. Plaintiff Diaab suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Plaintiff Diaab's Private Information is a form of intangible property that she entrusted to Defendant.

218. Plaintiff Diaab has suffered (and will continue to suffer) imminent and impending injuries from the substantially increased risk of fraud, identity theft, and misuse of her Private Information—all because Defendant exposed her Private Information to criminals.

219. Plaintiff Diaab has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

220. Plaintiff Diaab receives spam calls and texts following the data breach, showing that her information is being misused to persistently contact her with unwanted solicitations.

221. Plaintiff Diaab suffered concrete and substantial injuries because of Defendant's misconduct. Specifically, her finances were assaulted by a string of fraudulent activity and theft. And so, Plaintiff Diaab has spent day after day struggling to secure her identity and salvage her finances.

222. Plaintiff Diaab is a preschool teacher. But Plaintiff Diaab was forced to leave her

students to deal with the issues caused by the barrage of identity theft and fraudulent charges.

223. Two bank accounts were fraudulently opened in Plaintiff Diaab's name (one from Navy Federal and one from Quontic Bank).

224. In addition, a host of fraudulent charges were made on Plaintiff Diaab's M&T Bank checking account.

225. Plaintiff Diaab also experienced fraudulent charges on her Santander credit card account.

226. In short, the fallout of Defendant's data breach rippled throughout Plaintiff Diaab's life, wreaking havoc. The result is one inescapable conclusion: Defendant inflicted concrete and substantial injuries on Plaintiff Diaab.

IV. CLASS ALLEGATIONS

227. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

228. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **All persons residing in the United States whose Private Information was compromised in the data breach announced by MMC in August 2022. (the "Class").**

229. Excluded from the Class are the following individuals and/or entities: MMC, and MMC's parents, subsidiaries, affiliates, officers and directors, and any entity in which MMC has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections,

groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

230. Plaintiffs reserve the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

231. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in Data Breach. Defendant reported to the Attorney General of Maine that the Data Breach affected 191,752 individuals.

232. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

233. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

234. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

235. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the

same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

236. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

237. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

238. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because MMC would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered;

proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

239. The litigation of the claims brought herein is manageable. MMC's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

240. Adequate notice can be given to Class Members directly using information maintained in MMC's records.

241. Unless a Class-wide injunction is issued, MMC may continue in its failure to properly secure the Private Information of Class Members, MMC may continue to refuse to provide proper notification to Class Members regarding the Data Breach, the Private Information MMC continues to maintain will remain at risk of future breach, and MMC may continue to act unlawfully as set forth in this Complaint.

242. Further, MMC has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to the Class Members as a whole is appropriate.

243. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise

due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information; and/or

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

244. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

245. Plaintiffs and Class Members entrusted their Private Information to Defendant.

Defendant owed to Plaintiffs and other Class Members a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

246. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their Private Information in accordance with industry standards concerning data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

247. Defendant owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

248. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols.

Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

249. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

250. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

251. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

252. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiffs and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

253. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and

remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

254. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

255. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

256. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect individuals' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and Class Members' sensitive Private Information.

257. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

258. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

259. Defendant had a duty to Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and Class Members' Private Information.

260. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

261. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

262. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

263. The injury and harm suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Private Information.

264. Had Plaintiffs and Class Members known that Defendant did not adequately protect their Private Information, Plaintiffs and Class Members would not have entrusted Defendant with their Private Information.

265. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Private Information; unreimbursed losses relating to fraudulent charges; losses

relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

266. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

267. Plaintiffs bring this claim for unjust enrichment in the alternative to Plaintiffs' claims for breach of contract.

268. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for providing education or employment to current and former students and employees.

269. Plaintiffs and Class Members also conferred a monetary benefit on Defendant in the form of their Private Information, from which Defendant derived revenue as it could not provide education, employment, or services without the use of that Private Information.

270. Defendant collected, maintained, and stored Plaintiffs and Class Members' Private Information and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiffs and Class Members.

271. The money that Plaintiffs and Class Members paid to Defendant, or the revenue Defendant derived from the use of their Private Information, should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' Private Information. Additionally,

employees conferred a monetary benefit on Defendant as part of their salary and benefits was intended to apply to adequate data security which Defendant did not apply.

272. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive Private Information, as evidenced by the Data Breach.

273. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive Private Information, Plaintiffs and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' Private Information.

274. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' Private Information.

275. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of Private Information, loss of privacy, and a present increased risk of harm.

COUNT IV
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

276. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

277. Plaintiffs and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between themselves and Defendant, contracts that (upon information and belief) include obligations to keep sensitive Private Information confidential and secure.

278. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit Plaintiffs and the Class, as Defendant's service was to provide education services in exchange for tuition payments from Plaintiffs and the Class, but also safeguarding the Private Information entrusted to Defendant in the process of providing these services, applying for those services, or applying for and/or accepting employment.

279. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiffs' and Class Members' Private Information and to timely and accurately disclose the Data Breach to Plaintiffs and Class Members

280. Defendant materially breached its contractual obligation to protect the Private Information of Plaintiffs and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

281. Defendant materially breached its contractual obligations to Plaintiffs and the Class by failing to timely notify them of the breach, failing to disclose the precise Private Information impacted by the Data Breach, and failing to disclose the other details that it did disclose in its Notice Letters to the Attorneys General and certain Class Members.

282. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

283. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their Private Information, the loss of control of their Private Information, the present risk of suffering additional damages, and out-of-pocket expenses.

284. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

285. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

286. Plaintiffs' and Class Members' Private Information was provided to Defendant as part of education services or employment that Defendant provided to Plaintiffs and Class Members.

287. Plaintiffs and Class Members agreed to pay Defendant tuition for education and administration services. Additionally, applicants for admission or employment agreed to provide their Private Information in exchange for Defendant's promise to keep it safe from unauthorized access.

288. Defendant's Privacy Statement, posted on its website, represents that it "provides a secure server to protect [students'] information. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure information. The Information Technology department at Marymount Manhattan employs various measures to protect the

security of its computing resources and its users' accounts "take[s] great effort to protect patient confidentiality and privacy."[66]

289. In its Information Technology Policy, posted on its website, Defendant

a. represents that it "will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives," including as to "[a]ll information stored on applicable information systems."[67]

b. represents that it "safeguards the privacy of students, employees, College business, and other matters by protecting electronic records classified as confidential information."[68]

c. recognizes that it "should gather as little information as possible for legitimate purposes and delete information when it is no longer needed or no longer required by law to be retained."[69]

290. Defendant's Information Security Plan, posted on its website, provides that "covered data," including Social Security numbers, will be protected by "reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly."[70]

291. Defendant and Plaintiffs and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiffs' and Class Members' Private Information, whereby, Defendant was obligated

[66] Exhibit 1.
[67] Exhibit 2 § 1.4.
[68] *Id.* § 17.
[69] *Id.* § 17.7.
[70] Exhibit 3 §§ 2, 4.3.

to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' Private Information.

292. Defendant had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used in accordance with its contractual obligations.

293. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' Private Information and to comply with industry standards and applicable laws and regulations for the security of this information.

294. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information.

295. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

296. Defendant further breached the implied contract by providing untimely notification to Plaintiffs and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

297. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

298. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

299. Had Defendant disclosed that its data security was inadequate, neither Plaintiffs or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

300. As a result of Data Breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their Private Information, as well as the loss of control of their Private Information, and remain at present risk of suffering additional damages.

301. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT VI
Violations of the New York General Business Law § 349
(On Behalf of Plaintiffs and the Class)

302. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

303. Defendant's Information Technology Department is located on the 4th floor of Carson Hall at Defendant's campus in New York, New York.[71]

304. Defendant's Privacy Statement, posted on its website, represents that it "provides a secure server to protect your information. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure information. ***The Information Technology department at Marymount Manhattan*** employs various measures to protect the security of its computing resources and its users' accounts."[72]

[71] *See* https://www.mmm.edu/offices/information-technology/ (last accessed Aug. 16, 2022).
[72] Exhibit 1 (emphasis added).

305. The Privacy Statement directs questions about the Privacy Notice or Defendant's "data collection practices" to (i) the Executive VP of Financial and Administration and CFO and (ii) the Assistant Vice President for Information Technology.

306. The Information Technology Department is responsible for the accuracy of the representations made in the Privacy Statement.

307. The Information Technology Department is responsible for protecting the Private Information of Plaintiffs and Class Members, including providing a secure server for the Private Information and putting in place appropriate physical, electronic, and managerial procedures to safeguard and secure the Private Information.

308. The Privacy Statement represents that Defendant "provides a secure server to protect [students'] information. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure information. The Information Technology department at Marymount Manhattan employs various measures to protect the security of its computing resources and its users' accounts "take[s] great effort to protect patient confidentiality and privacy."[73]

309. In its Information Technology Policy, posted on its website, Defendant

a. represents that it "will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives," including as to "[a]ll information stored on applicable information systems."[74]

b. represents that it "safeguards the privacy of students, employees, College

[73] *Id*.
[74] Exhibit 2 § 1.4.

business, and other matters by protecting electronic records classified as confidential information."[75]

c. recognizes that it "should gather as little information as possible for legitimate purposes and delete information when it is no longer needed or no longer required by law to be retained."[76]

310. Defendant's "Information Protection Committee (IPC) is responsible and accountable for ensuring that the objectives of the security policy are met."[77]

311. Defendant's "Chief Information Officer is responsible for implementation of the policy."[78]

312. Defendant's Information Security Plan, posted on its website, provides that "covered data," including Social Security numbers, will be protected by "reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly."[79]

313. Defendant's Chief Information Officer is responsible for implementing and maintaining the Information Security Plan.[80]

314. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. L. § 349(a), including but not limited to the following:

---

[75] *Id.* § 17.
[76] *Id.* § 17.7.
[77] *Id.* § 1.5.
[78] *Id.*
[79] Exhibit 3 §§ 2, 4.3.
[80] *Id.* § 4.1.

a. Misrepresenting that it would use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives;

b. Misrepresenting that it would sufficiently protect the Private Information entrusted to it;

c. Misrepresenting that it would delete Private Information it no longer had a reasonable need to maintain—here, Defendant has maintained at least one victim's Private Information (i.e., Plaintiff Marano's) for more than twenty years since she was last a student;

d. Misrepresenting that it would implement reasonable safeguards to control identified risks to the security, confidentiality, and integrity of the Private Information; and

e. Misrepresenting that it would regularly monitor the effectiveness of these safeguards.

315. Defendant knew (or should have known) that its computer systems and data security practices were inadequate to safeguard the Private Information entrusted to it—such that the risk of a data breach and or theft was highly likely.

316. Defendant should have disclosed this information because it was in a superior position to know the true facts related to the defective data security.

317. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendant's network and aggregation of Private Information.

318. The representations which consumers (including Plaintiffs and Class Members) relied upon were material representations—e.g., relating to Defendant's adequate protection of Private Information—such that consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

319. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members were harmed—in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

320. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs and Class Members' Private Information was disclosed to third parties without authorization, which has caused and will continue to cause damage to Plaintiffs and Class Members.

321. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT VII
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

322. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

323. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and violate the federal and state statutes described above.

324. An actual controversy has arisen—because of the data breach at issue—regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remains inadequate and unreasonable. Additionally, Plaintiffs and Class Members continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

325. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

326. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the Private Information with which it is entrusted, and to notify impacted individuals of the data breach under the common law and Section 5 of the FTC Act;

327. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure the Private Information entrusted to it; and

328. Defendant's breach of its legal duty continues to harm Plaintiffs and Class Members.

329. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the data of Plaintiffs and Class Members that remains in its possession and is subject to the risk of further data breaches.

330. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily

quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and Class Members for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and Class Members, which include monetary damages that are not legally quantifiable or provable.

331. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

332. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

COUNT VIII
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

333. Plaintiffs and Class Members incorporate the above allegations as if fully set forth herein.

334. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

335. Defendant owed a duty to Plaintiffs and Class Members to keep this information confidential.

336. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

337. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

338. The data breach constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

339. Defendant acted with a knowing state of mind when it permitted the data breach because it knew its information security practices were inadequate.

340. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the data breach, thereby materially impairing their mitigation efforts.

341. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

342. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and Class Members to suffer damages.

343. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

344. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A

judgment for monetary damages will not end Defendant's inability to safeguard their Private Information.

345. In addition to injunctive relief, Plaintiffs, on behalf of herself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

346. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the MMC and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and their Counsel to represent the certified Class;

B. For equitable relief enjoining MMC from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' Private Information, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and the Class;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including but not limited to an order:

i. prohibiting MMC from engaging in the wrongful and unlawful acts described

herein;

ii. requiring MMC to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring MMC to delete, destroy, and purge the personal identifying information of Plaintiffs and Class unless MMC can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class;

iv. requiring MMC to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and Class Members' personal identifying information;

v. prohibiting MMC from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring MMC to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on MMC's systems on a periodic basis, and ordering MMC to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring MMC to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring MMC to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring MMC to segment data by, among other things, creating firewalls and access controls so that if one area of MMC's network is compromised, hackers cannot gain access to other portions of MMC's systems;

x. requiring MMC to conduct regular database scanning and securing checks;

xi. requiring MMC to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring MMC to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring MMC to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with MMC's policies, programs, and systems for protecting personal identifying information;

xiv. requiring MMC to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor MMC's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring MMC to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring MMC to implement logging and monitoring programs sufficient to track traffic to and from MMC's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate MMC's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: October 21, 2022

Respectfully Submitted,

s/ Blake Hunter Yagman

Blake Hunter Yagman
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
byagman@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

Terence R. Coates (*Pro Hac Vice)*
Justin C. Walker (*Pro Hac Vice)*
Jonathan T. Deters *
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com

Jonathan M. Sedgh
MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
Email: jsedgh@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Phone: (608) 237-1775
Fax: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice applications forthcoming*